CyberRisk – Prinzip Hoffnung

Obwohl viele Mittelständler in der Corona-Pandemie auf Homeoffice und mobiles Arbeiten angewiesen sind, sind sie auf Cyber-Attacken nicht vorbereitet!

48% der Mittelständler haben KEINEN **NOTFALLPLAN** für den Fall einer Cyber-Attacke

58% könnten bei einem Ausfall ihrer IT-Systeme aber **KAUM NOCH ARBEITEN**

In 44% der befragten Unternehmen ist **NIEMAND** für die **Sicherheit der IT Systeme** verantwortlich

58% der Cyberattacken sind **ERFOLGREICH,** weil Mitarbeiter **verseuchte Anhänge** öffnen oder **schädliche Links anklicken**

69% bieten den eigenen Mitarbeitern **KEINE IT-/Datenschutz-Schulungen** an

Nach einem Cyber-Angriff gelang es nur 1/3 der Betroffenen die IT-Systeme **innerhalb EINES TAGES** wieder zum laufen zu bringen

Jedes **fünfte** Unternehmen benötigt dafür **mehr als DREI TAGE**

Nach Umfragen erledigen knapp 60 Prozent der Angestellten ihre beruflichen Aufgaben mit privaten Laptops, Tablets oder Smartphones. Private Geräte und E-Mail -Accounts sind in der Regel schlechter geschützt als die firmeneigene IT. Dadurch verlieren Unternehmen die Kontrolle über Ihre IT-Sicherheit und damit über die Sicherheit ihrer Daten.

Die Gangster sind also perfide, die Unternehmer und Mitarbeiter viel zu sorglos – und auf eine Cyber-Attacke nicht vorbereitet. Viele Unternehmen reagieren auf einen Cyber-Angriff plan- und kopflos. Das kostet im Ernstfall viel Geld, weil es länger dauert, bis die IT-Systeme gesäubert und die Daten wieder ehrgestellt sind.

Während 2019 die durchschnittlichen Cyber-Schadenkosten international noch bei 9.000 € lagen, sind sie rapide gestiegen: 2020 lagen sie im Schnitt bei 51.200 €, in Deutschland sogar noch rund 20.000 € höher – und deutsche Firmen werden noch dazu von den global agierenden Hackern besonders häufig angegriffen.